UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/558,629	11/30/2005	Katsunori Matsuura	281486US90PCT	4628

22850 7590 10/06/2009		

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
AMPAGOOMIAN, DAVID S

ART UNIT	PAPER NUMBER
2446	

NOTIFICATION DATE	DELIVERY MODE
10/06/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/558,629	MATSUURA, KATSUNORI
	Examiner	Art Unit
	DAVID AMPAGOOMIAN	2446

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>30 November 2005</u>.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-28</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) <u>1-28</u> is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on <u>30 November 2005</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☒ All   b) ☐ Some * c) ☐ None of:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. _____.
    3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)
1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>05/11/2009, 02/12/2008, 11/30/2005</u>.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

DETAILED ACTION

Claims 1-28 are pending.

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2.   **Claims 6-7, 17-18 and 21 are rejected under 35 U.S.C. 102(e) as being**

anticipated by Chang et al. (US 2004/0100976) hereafter Chang.

        Regarding claim 6, Chang discloses an address translation apparatus for a

terminal or a server on a private network that does not have an address on a global

network to perform communication through the global network, comprising:

        a WAN interface unit which provides communication with the global network

("public network 100" Chang: [0024] and fig. 1);

        a LAN interface unit which provides communication with the private network ("a

private network 101 Chang: [0024] and fig. 1);

        an address translation unit having (Chang: [0024]):

means for translating an address in accordance with an address translation rule established on a per sending device basis("FIG. 4 shows the format of the NAPT table in accordance with the present invention" Chang: [0022]),

in order to transferring information from a terminal on the global network to a terminal on the private network (Chang: [0026], [0022], [0031], [0007]); and

means for translating an address in accordance with an address translation rule established on a per sending device basis (Chang: [0026-0037], [0007]), in order to transferring information from a terminal on the private network to a terminal on the global network (Chang: [0026-0037],[0007]); and

a database unit for recording the address translation rules (Chang: [0026-0037], [0007]).

Regarding claim 7, Chang discloses the address translation apparatus according to Claim 6 as described above. Chang further disclose, wherein the address translation unit further has : means for adding an address translation rule established on a per sending device basis to the database unit in response to a request for initiating communication sent from a terminal on the global network or a terminal on a private network (Chang: [0026-0037], [0007]); and

means for deleting the added address translation rule from the database unit when a predetermined criterion for ending communication is satisfied ("lifetime 302 represents the time that the connection-related NAPT data remains in the table" Chang: [0026-0037], [0007]).

Regarding claim 17, Chang discloses the address translation apparatus according to Claim 6 as described above. Chang further discloses, comprising: the address translation rule has a condition with the IP address of the sending device or the IP address of the sending network (Chang: [0026-0037], [0007]).

Regarding claim 18, Chang discloses the address translation apparatus according to Claim 17 as described above. Chang further discloses wherein the address translation unit further has: means for adding an address translation rule established on a per sending device basis to the database unit in response to a request for initiating communication sent from a terminal on the global network or a terminal on a private network (Chang: [0026-0037], [0007]); and means for deleting the added address translation rule from the database unit when a predetermined criterion for ending communication is satisfied ("lifetime 302 represents the time that the connection-related NAPT data remains in the table" Chang: [0026-0037], [0007])..

Regarding claim 21, an address translation method for a terminal on a private network that does not have an address on a global network to perform communication through the global network, comprising:

recording an address translation rule established on a par sending device basis in a database unit beforehand ("FIG. 4 shows the format of the NAPT table in accordance with the present invention" Chang: [0022]);

when a packet from the global network is received by a WAN interface unit

("public network 100" Chang: [0024] and fig. 1), translating, by an address translation

unit, a destination address in accordance with the address translation rule; and

transferring, by a LAN interface unit, the packet having the translated address to

the private network(Chang: [0026-0037], [0007]);

when a packet from the private network is received by a LAN interface unit ("a

private network 101 Chang: [0024] and fig. 1),

translating, by the address translation unit, a source address in accordance with the

address translation rule (Chang: [0026-0037], [0007]); and

transferring, by the WAN interface unit, the packet having the translated address

to the global network(Chang: [0026-0037], [0007]).

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 1-5, 8-16, 19-20 and 22-28 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Chang et al. (US 2004/0100976) hereafter Chang in view

of Kokado et al. (US 2003/0115327) hereafter Kokado.

Regarding claim 1, Chang discloses a relay apparatus for a terminal or a server on a private network that does not have an address on a global network to perform communication through the global network, comprising:

a WAN interface unit which provides communication with the global network ("public network 100" Chang: [0024] and fig. 1);

a LAN interface unit which provides communication with the private network ("a private network 101" Chang: [0024] and fig. 1);

an address translation unit having (Chang: [0024]):

means for translating an address in accordance with an address translation rule established on a per sending device basis ("FIG. 4 shows the format of the NAPT table in accordance with the present invention" Chang: [0022]), in order to transferring information from a terminal on the global network to a terminal on the private network (Chang: [0026], [0022], [0031], [0007]); and

means for translating an address in accordance with an address translation rule established on a per sending device basis (Chang: [0026-0037], [0007]), in order to transferring information from a terminal on the private network to a terminal on the global network (Chang: [0026-0037],[0007]); and

a database unit which records the access control rule and the address translation rule (Chang: [0026-0037], [0007]).

Chang does not explicitly disclose an access control unit having means for controlling access from the global network to the private network in accordance with an

access control rule which is established on a per sending device basis or on a per sending network basis.

However Kokado discloses a method firewall system to control access from an internal private network and an external public network based on a per sending device basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-0010]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to create network address translation of Chang to include the access control method of Kokado in order to prevent unauthorized access to the private network (Kokado: [0002-0010]).

Regarding claim 2, the modified Chang reference discloses the relay apparatus according to Claim 1 as described above. Chang does not explicitly disclose, comprising: an authentication unit which performs authentication in response to a request for access permission sent from a terminal on the global network, wherein: the database unit further records user information used by the authentication unit to perform authentication; the access control unit further has: means for adding an access control rule established on a per sending device basis or a per sending network basis to the database unit if the authentication succeeds; and means for deleting the added access control rule from the database unit when a predetermined criterion for ending communication is satisfied; and the address translation unit further has: means for

adding an address translation rule established on a per sending device basis to the

database unit if the authentication succeeds; and means for deleting the added address

translation rule from the database unit when a predetermined criterion for ending

communication is satisfied.

However Kokado discloses a method firewall system to control access from an

internal private network and an external public network based on a per sending device

basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and

Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-

0010]). Kokado further discloses the use authentication function and database for

storing access control rules (Kokado: [0019-0021]). Kokado also discloses deleting the

added address translation rule from the database unit when a predetermined criterion

for ending communication is satisfied (Kokado: [0049]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to create network address translation of Chang to include the access control

and authentication method of Kokado in order to prevent unauthorized access to the

private network (Kokado: [0002-0010])

Regarding claim 3, the modified Chang reference discloses relay apparatus

according to Claim 1 as described above. Kokado further discloses, wherein: the

access control unit further has: means for adding an access control rule established on

a per sending device basis or on a per sending network basis to the database unit in

response to a request from an authentication sever which performs authentication of a

terminal on the global network (Kokado: [0019-0021]); and means for deleting the

added access control rule from the database unit when a predetermined criterion for

ending communication is satisfied (Kokado: [0048-0049]; fig. 8).; and the address

translation unit further has: means for adding an address translation rule established on

a per sending device basis to the database unit in response to a request from the

authentication server(Kokado: [0073]; [0032-0034]); and means for deleting the added

address translation rule from the database unit when a predetermined criterion for

ending communication is satisfied (Kokado: [0048-0049]; fig. 8).

Regarding claim 4, the modified Chang reference discloses an authentication

server which permits access to the relay apparatus according to Claim 3 as described

above. Kokado further disclose, comprising: an interface unit which provides

communication with a terminal on the global network and the relay apparatus (Kokado:

[0003]); an authentication unit which performs authentication in response to a request

for permission to access the relay apparatus from a terminal on the global

network(Kokado: [0019-0021]); a control unit having: means for requesting the relay

apparatus to add an access control rule and an address translation rule for a packet

from a terminal on the global network if authentication at the authentication unit

succeeds (Kokado: [0019-0021]); and means for requesting the relay apparatus to

delete the added access control rule and address translation rule when a predetermined

criterion for ending communication is satisfied (Kokado: [0188]; [0190-0191]; [0116])

and Figures 9-10 and 22); and a database unit which records information associating

user information used by the authentication unit to perform authentication with an access control rule and address translation rule requested to be added (Kokado: [0188]; [0190-0191]; [0116]) and Figures 9-10 and 22).

Regarding claim 5, the modified Chang reference discloses the relay apparatus according to 1 as described above, wherein: the access control unit further has: means for adding an access control rule established on a per sending device basis to the database unit in response to a request for initiating communication from a terminal on a private network (Kokado: [0188]; [0190-0191]; [0116]) and Figures 9-10 and 22); and means for deleting the added access control rule from the database unit when a predetermined criterion for ending communication is satisfied (Kokado: [0048-0049]; fig. 8); and the address translation unit further has: means for adding an address translation rule established on a per sending device basis to the database unit in response to a request for initiating communication from a terminal on the private network (Kokado: [0033]; [0117]); and means for deleting the added address translation rule from the database unit when a predetermined criterion for ending communication is satisfied (Kokado: [0048-0049]; fig. 8).

Regarding claim 8, Change discloses the address translation apparatus according to Claim 7 as described above. Change does not explicitly disclose, comprising: an authentication unit which performs authentication in response to a

request for initiating communication from a terminal on the global network, wherein: the

database unites further records user information used by the authentication unit to

perform authentication; and the address translation unit adds the address translation

rule to the database unit in response to a request for initiating communication from a

terminal on the global network only if the authentication succeeds.

However Kokado discloses a method firewall system to control access from an

internal private network and an external public network based on a per sending device

basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and

Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-

0010]). Kokado further discloses the use authentication function and database for

storing access control rules (Kokado: [0019-0021]). Kokado also discloses the use of

address translation rules from the database unit (Kokado: [0049]; [0165-0167]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to create network address translation of Chang to include the access control

and authentication method of Kokado in order to prevent unauthorized access to the

private network (Kokado: [0002-0010])

Regarding claim 9, Change discloses the address translation apparatus

according to Claim 7 as described above. Change does not explicitly disclose, wherein

the address translation unit adds the address translation rule to the database unit in

response to a request for initiating communication from a terminal on the global network

only if an authentication server which performs authentication requests the addition.

However Kokado discloses a method firewall system to control access from an internal private network and an external public network based on a per sending device basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-0010]). Kokado further discloses the use authentication function and database for storing access control rules (Kokado: [0019-0021]). Kokado also discloses the use of address translation rules from the database unit (Kokado: [0049]; [0165-0167]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to create network address translation of Chang to include the access control and authentication method of Kokado in order to prevent unauthorized access to the private network (Kokado: [0002-0010]).

Regarding claim 10, Change discloses the address translation apparatus according to Claim 9 as described above. Change does not explicitly disclose an authentication server which permits access to the address translation apparatus, comprising: an interface unit which provides communication with a terminal on the global network and the address translation apparatus; an authentication unit which performs authentication in response to a request for permission to access the address translation apparatus from a terminal on the global network; a control unit having: means for requesting the address translation apparatus to add an address translation rule for a packet sent from a terminal on the global network if authentication at the

authentication unit succeeds; and means for requesting the address translation apparatus to delete the added address translation rule when a predetermined criterion for ending communication is satisfied; and a database unit which records user information used by the authentication unit to perform authentication.

However Kokado discloses a method firewall system to control access from an internal private network and an external public network based on a per sending device basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-0010]). Kokado further discloses the use authentication function and database for storing access control rules (Kokado: [0019-0021]). Kokado also discloses the use of address translation rules from the database unit (Kokado: [0049]; [0165-0167]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to create network address translation of Chang to include the access control and authentication method of Kokado in order to prevent unauthorized access to the private network (Kokado: [0002-0010])

Regarding claim 11, Chang disclose a firewall apparatus which allows a packet from a global network external to the firewall to pass through to a private network internal to the firewall apparatus if the packet meets an acceptance condition set in a database unit, comprising:

a WAN interface unit which provides communication with the global network ("public network 100" Chang: [0024] and fig. 1);

a LAN interface unit which provides communication with the private network ("a

private network 101 Chang: [0024] and fig. 1);

Chang does not explicitly disclose an access control unit having means for

controlling access from the global network to the private network in accordance with an

access control rule established on a per sending device basis or on a per sending

network basis ; an authentication unit which performs authentication in response to a

request for access permission from the global network; and a database unit which

records the access control rule and user information used by the authentication unit to

perform authentication.

However Kokado discloses a method firewall system to control access from an

internal private network and an external public network based on a per sending device

basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and

Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-

0010]). Kokado further discloses the use authentication function and database for

storing access control rules (Kokado: [0019-0021]). Kokado also discloses the use of

address translation rules from the database unit (Kokado: [0049]; [0165-0167]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to create network address translation of Chang to include the access control

and authentication method of Kokado in order to prevent unauthorized access to the

private network (Kokado: [0002-0010])

Regarding claim 12, the modified Chang reference discloses the firewall apparatus according to Claim 11 as described above. Chang does not explicitly disclose , wherein: the access control unit further has means for adding an access control rule established on a per sending device basis or on a per sending network basis to the database unit if authentication at the authentication unit succeeds and an access control rule for a request for access permission from a device on the global network is not recorded in the database unit; and means for deleting the added access control rule from the database unit when a predetermined criterion for ending communication is satisfied.

However Kokado discloses a method firewall system to control access from an internal private network and an external public network based on a per sending device basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-0010]). Kokado further discloses the use authentication function and database for storing access control rules (Kokado: [0019-0021]). Kokado also discloses deleting the added address translation rule from the database unit when a predetermined criterion for ending communication is satisfied (Kokado: [0049]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to create network address translation of Chang to include the access control and authentication method of Kokado in order to prevent unauthorized access to the private network (Kokado: [0002-0010])

Regarding claim 13, the modified Chang reference discloses the firewall apparatus according to Claim 12 as described above. Chang does not explicitly wherein the access control unit further has: means for, if a request for new access permission is provided from a device on the global network that is using an established secure session during the duration of the secure session, sending notification seeking confirmation of the request to the device on the global network by using the secure session; and means for rejecting a new access regardless of the access control rule if denial of the request is returned from the device on the global network.

However Kokado discloses a method firewall system to control access from an internal private network and an external public network based on a per sending device basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-0010]). Kokado further discloses the use authentication function and database for storing access control rules (Kokado: [0019-0021]). Kokado also discloses the use of address translation rules from the database unit (Kokado: [0049]; [0165-0167]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to create network address translation of Chang to include the access control and authentication method of Kokado in order to prevent unauthorized access to the private network (Kokado: [0002-0010])

Regarding claim 14, the modified Chang reference the firewall apparatus according to Claim 11 as described above. Chang does not explicitly disclose wherein

the access control unit further has: means for monitoring the status of communication; and means for notifying the device on the global network of an anomaly in communication if a predetermined criterion for communication anomaly is satisfied. However Kokado disclose a method of monitoring the status of communication (Kokado: [0050], [0171]); means for notifying the device on the global network of an anomaly in communication if a predetermined criterion for communication anomaly is satisfied (Kokado: [0094]; [0171]; [0186]).

Regarding claim 15, the modified Chang reference discloses relay apparatus according to Claim 1 as described above. Chang does not explicitly disclose , comprising: the access control rule and the address translation rule have a condition with the IP address of the sending device or the IP address of the sending network.

However Kokado discloses a method firewall system to control access from an internal private network and an external public network based on a per sending device basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-0010]). Kokado further discloses the use authentication function and database for storing access control rules (Kokado: [0019-0021]). Kokado also discloses the use of address translation rules from the database unit (Kokado: [0049]; [0165-0167]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to create network address translation of Chang to include the access control

and authentication method of Kokado in order to prevent unauthorized access to the

private network (Kokado: [0002-0010])

Regarding claim 16, the modified Chang reference discloses relay apparatus

according to Claim 15 as described above. Chang does not explicitly , comprising:

an authentication unit which performs authentication in response to a request for access

permission sent from a terminal on the global network, wherein: the database unit

further records user information used by the authentication unit to perform

authentication; the access control unit further has: means for adding an access control

rule established on a per sending device basis or a per sending network basis to the

database unit if the authentication succeeds; and means for deleting the added access

control rule from the database unit when a predetermined criterion for ending

communication is satisfied; and the address translation unit further has: means for

adding an address translation rule established on a per sending device basis to the

database unit if the authentication succeeds; and means for deleting the added address

translation rule from the database unit when a predetermined criterion for ending

communication is satisfied.

However Kokado discloses a method firewall system to control access from an

internal private network and an external public network based on a per sending device

basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and

Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-

0010]). Kokado further discloses the use authentication function and database for

storing access control rules (Kokado: [0019-0021]). Kokado also discloses the use of

address translation rules from the database unit (Kokado: [0049]; [0165-0167]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to create network address translation of Chang to include the access control

and authentication method of Kokado in order to prevent unauthorized access to the

private network (Kokado: [0002-0010])

Regarding claim 19, the modified Chang reference disclose the firewall

apparatus according to Claim 11 as described above. Chang does not explicitly

disclose, comprising: the access control rule has a condition with the IP address of the

sending device or the IP address of the sending network.

However Kokado discloses a method firewall system to control access from an

internal private network and an external public network based on a per sending device

basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and

Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-

0010]). Kokado further discloses the use authentication function and database for

storing access control rules (Kokado: [0019-0021]). Kokado also discloses the use of

address translation rules from the database unit (Kokado: [0049]; [0165-0167]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to create network address translation of Chang to include the access control

and authentication method of Kokado in order to prevent unauthorized access to the

private network (Kokado: [0002-0010])

Regarding claim 20, the modified Chang reference disclose the firewall

apparatus according to Claim 19 as described above. Chang does not explicitly

wherein: the access control unit further has means for adding an access control rule

established on a per sending device basis or on a per sending network basis to the

database unit if authentication at the authentication unit succeeds and an access control

rule for a request for access permission from a device on the global network is not

recorded in the database unit; and means for deleting the added access control rule

from the database unit when a predetermined criterion for ending communication is

satisfied.

However Kokado discloses a method firewall system to control access from an

internal private network and an external public network based on a per sending device

basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and

Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-

0010]). Kokado further discloses the use authentication function and database for

storing access control rules (Kokado: [0019-0021]). Kokado also discloses deleting the

added address translation rule from the database unit when a predetermined criterion

for ending communication is satisfied (Kokado: [0049]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to create network address translation of Chang to include the access control

and authentication method of Kokado in order to prevent unauthorized access to the

private network (Kokado: [0002-0010])

Regarding claim 22, Chang discloses an address translation method for a terminal on a private network that does not have an address on a global network to perform communication through the global network, comprising:

recording an address translation rule established on a per sending device basis in a database unit beforehand ("FIG. 4 shows the format of the NAPT table in accordance with the present invention" Chang: [0022]);

when a packet from the global network is received by a WAN interface unit ("public network 100" Chang: [0024] and fig. 1),

if a matching address translation rule is not found in the database unit, adding an address translation rule to the database unit and translating the address of the packet in accordance with the added address translation rule (Chang: [0026-0037], [0007]); and

transferring, by a LAN interface unit, the packet having the translated address to the private network ("a private network 101" Chang: [0024] and fig. 1; Chang: [0026], [0022], [0031], [0007]);

when a packet from the private network is received by the LAN interface unit; checking, by the address translation unit, the database unit to see whether or not an address translation rule that matches source information and destination information of the packet is recorded in the database unit (Chang: [0026], [0022], [0031], [0007]), and

if a matching address translation rule is found in the database unit, translating the

address of the packet in accordance with the address translation rule (Chang: [0026-

0037], [0007]);

if a matching address translation rule is not found in the database unit, adding an

address translation rule to the database unit and translating the address of the packet in

accordance with the added address translation rule (Chang: [0026-0037], [0007]); and

transferring by the WAN interface unit the packet having the translated address

to the global network(Chang: [0026-0037], [0007]); and

if there is an address translation rule added by the address translation unit,

deleting the address translation rule from the database unit when a predetermined

criterion for ending communication is satisfied ("lifetime 302 represents the time that the

connection-related NAPT data remains in the table 106" Chang:[0031]).

Chang does not explicitly disclose performing authentication in an authentication

unit and if f the authentication succeeds, checking, by the address translation unit, the

database unit to see whether or not an address translation rule that matches source

information and destination information of the packet is stored in the database unit, and

if a matching address translation rule is found in the database unit, translating the

address of the packet in accordance with the address translation rule;

However Kokado discloses a method firewall system to control access from an

internal private network and an external public network based on a per sending device

basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and

Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-

0010]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to create network address translation of Chang to include the access control

method of Kokado in order to prevent unauthorized access to the private network

(Kokado: [0002-0010]).

Regarding claim 23, the modified Chang reference discloses the address

translation method according to Claim 22 as described above. Chang does not

explicitly disclose, wherein, instead of performing authentication in the authentication

unit, determination is made that authentication is successful when a request is received

from an authentication server which performs authentication of a terminal on the global

network. However Kokado discloses a method firewall system to control access from an

internal private network and an external public network based on a per sending device

basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and

Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-

0010]). Kokado further discloses the use authentication function and database for

storing access control rules (Kokado: [0019-0021]). Kokado also discloses deleting the

added address translation rule from the database unit when a predetermined criterion

for ending communication is satisfied (Kokado: [0049]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to create network address translation of Chang to include the access control

and authentication method of Kokado in order to prevent unauthorized access to the

private network (Kokado: [0002-0010])

Regarding claim 24, Change discloses an access control method for allowing a

packet from a global network external to a firewall to pass through to a private network

internal to the firewall if the packet meets an access control rule set in a database unit,

comprising:

recording an access control rule established on per a sending device basis or on

a per sending network basis in a database unit beforehand ("FIG. 4 shows the format of

the NAPT table in accordance with the present invention" Chang: [0022]); and

when a connection request from the global network is received by a WAN

interface unit, checking, by an access control unit, the database unit to see whether or

not an access control rule that matches the connection request is recorded in the

database unit ("public network 100" Chang: [0024] and fig. 1; Chang: [0026-0037],

[0007]). Chang does not explicitly disclose if the access control rule is found in the

database unit, permitting communication.

However Kokado discloses a method firewall system to control access from an

internal private network and an external public network based on a per sending device

basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and

Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-

0010]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to create network address translation of Chang to include the access control

method of Kokado in order to prevent unauthorized access to the private network

(Kokado: [0002-0010]).

Regarding claim 25, Chang discloses an access control method for allowing a

packet from a global network external to a firewall to pass through to a private network

internal to the firewall if the packet meets an access control rule set in a database unit,

comprising:

recording an access control rule established on a per sending device basis or on

a per sending network basis in a database unit beforehand ("FIG. 4 shows the format of

the NAPT table in accordance with the present invention" Chang: [0022]; [0026], [0022],

[0031], [0007]); and

when a connection request from the global network is received by a WAN

interface unit ("public network 100" Chang: [0024] and fig. 1),

if a matching access control rule is found in the database unit, permitting the

communication (Chang: [0026-0037], [0007]);

if a matching access control rule is not found in the database unit, adding an

access control rule established on a sending device basis or on a sending network

basis to the database unit and permitting the communication(Chang: [0026-0037],

[0007]);

when a packet from the private network is received by a LAN interface unit ,

checking, by the access control unit, the database unit to see whether or not an access

control rule that matches the connection request is recorded in the database

unit(Chang: [0026-0037], [0007]);

and if a matching access control rule is found in the database unit, permitting

communication(Chang: [0026-0037], [0007]).

Chang does not explicitly disclose performing authentication in an authentication

unit; and if the authentication succeeds, checking, by an access control unit, the

database unit to see whether or not an access control rule that matches the connection

request is recorded in the database unit; and if a matching access control rule is not

found in the database unit, adding an access control rule established on a sending

device basis to the database unit and permitting the communication; and if there is an

access control rule added by the access control unit, deleting the access control rule

from the database unit when a predetermined criterion for ending communication is

satisfied.

However Kokado discloses a method firewall system to control access from an

internal private network and an external public network based on a per sending device

basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and

Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-

0010]). Kokado further discloses the use authentication function and database for

storing access control rules (Kokado: [0019-0021]). Kokado also discloses deleting the

added address translation rule from the database unit when a predetermined criterion for ending communication is satisfied (Kokado: [0049]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to create network address translation of Chang to include the access control and authentication method of Kokado in order to prevent unauthorized access to the private network (Kokado: [0002-0010])

Regarding 26 claim, the modified Chang reference discloses the access control method according to Claim 25 as described above. Chang does not explicitly disclose, instead of performing authentication in the authentication unit, determination is made that authentication is successful when a request is received from an authentication server which performs authentication of a terminal on the global network.

However Kokado discloses a method firewall system to control access from an internal private network and an external public network based on a per sending device basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-0010]). Kokado further discloses the use authentication function and database for storing access control rules (Kokado: [0019-0021]). Kokado also discloses deleting the added address translation rule from the database unit when a predetermined criterion for ending communication is satisfied (Kokado: [0049]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to create network address translation of Chang to include the access control

and authentication method of Kokado in order to prevent unauthorized access to the

private network (Kokado: [0002-0010])

Regarding claim 27, the modified Chang reference discloses the access control

method according to Claim 24 as described above. Change does not explicitly disclose

, wherein: the communication status of a established secure session is monitored during

the secure session; and if a predetermined criterion is met, the device on the global

network that is using the established secure session is notified of occurrence of

anomaly. However Kokado disclose a method of monitoring the status of

communication (Kokado: [0050], [0171]); means for notifying the device on the global

network of an anomaly in communication if a predetermined criterion for communication

anomaly is satisfied (Kokado: [0094]; [0171]; [0186]).

Regarding claim 28, the modified Chang reference discloses the access control

method according to Claim 24 as described above. Change does not explicitly disclose

, wherein: if a new connection request from a terminal on the global network that has

established a secure session is received by the WAN interface unit during the duration

of the secure session, the information on the connection request is notified to the

terminal on the global network that has the established secure session; and if a denial

of the request is returned from the device, rejecting the connection regardless of the

access control rule recorded in the database unit.

However Kokado discloses a method firewall system to control access from an internal private network and an external public network based on a per sending device basis or on a per sending network basis (Kokado: [0188]; [0190-0191]; [0116]) and Figures 9-10 and 22) in order to provide security to the private network (Kokado: [0002-0010]). Kokado further discloses the use authentication function and database for storing access control rules (Kokado: [0019-0021]). Kokado also discloses deleting the added address translation rule from the database unit when a predetermined criterion for ending communication is satisfied (Kokado: [0049]). However Kokado disclose a method of monitoring the status of communication (Kokado: [0050], [0171]); means for notifying the device on the global network of an anomaly in communication if a predetermined criterion for communication anomaly is satisfied (Kokado: [0094]; [0171]; [0186]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to create network address translation of Chang to include the access control and authentication method of Kokado in order to prevent unauthorized access to the private network (Kokado: [0002-0010])

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID AMPAGOOMIAN whose telephone number is (571)270-1896. The examiner can normally be reached on Monday through Friday 9:30 AM to 7:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Jeffrey Pwu can be reached on 571-272-6798. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. A./
Examiner, Art Unit 2446

/Jeffrey Pwu/
Supervisory Patent Examiner, Art Unit 2446